A Survey about Blockchain Software Architectures

Amjad Aldweesh
Newcastle University
A.Y.A.Aldweesh2@ncl.ac.uk

Prof. Aad van Moorsel
Newcastle University
aad.vanmoorsel@ncl.ac.uk

Abstract

The key technique behind the Bitcoin is blockchain, which has emerged as great innovation with a wide range of applications. The blockchain is a public ledger or a public database that maintained by all participants of the Bitcoin network. All transactions that have ever occurred in the Bitcoin network are stored and recorded in the blockchain. The main feature of the blockchain is that it does not rely on a trusted third party, i.e. central trusted authority. This paper presents a survey about blockchain software architectures and the applications that benefit from this invention.

Keywords: *Blockchain, Security, Cryptocurrency, Smart Contracts*

1 Introduction

1.1 Background

The first and most popular cryptocurrency that has been receiving a lot of attention is bitcoin [1][2]. Enabling trust transactions without involving a trusted third party even if the participants do not trust each other is the technical feature of the Bitcoin. This feature is achieved by the invention of blockchain technology.

Blockchain is a public ledger where all transaction is recorded and shared by all nodes participating in the bitcoin network. The structure of the blockchain is that a block that consists of transactions is connected with the previous block in a chain from using a hash algorithm. To add a new block to the chain a process of solving a puzzle called proof-of-work (POW) or proof-of-stake (POS), which is not easy, is used and needed to ensure the reliability. POW can prevent attackers from forging the blockchain and avoid the double spending issue. Because the reliability of blockchain is securely kept on the large scale, use the discussions about the application rather than currency has been thrust into the spotlight. ”Bitcoin 2.0” is a given name for applications that benefit from the feature of the blockchain.

Blockchain can be classified into tow types namely public blockchain and private blockchain. The public blockchain is a blockchain that anyone in the world can read, send a transaction if it is valid and verify a block(e.g. bitcoin

blockchain). This type is useful when the participants of the network do not trust each other. The private blockchain is a blockchain where writing permissions are restricted to a centralised organisation. This blockchain can be used by an institution or consortium because it is easy to change the rules of the blockchain and revert transactions if needed.

1.2 Blockchain Applications

Blockchain has been utilised in some applications as follows.

- *Cryptocurrency:* To secure the transactions and control the monetary, cryptocurrency utilises cryptography. As mentioned above, the first and the most popular cryptocurrency is Bitcoin, which was created in 2008. Bitcoin has been utilised as asset and ownership registration rather than the transaction of monetary in Ascribe [2]. This is because adding 20-byte data to the transaction and recorded on the blockchain is allowed to developers.

  Cryptocurrencies such as coloured coins, which uses a subset of Bitcoin to represent and manage real-world assets, are overlay networks on Bitcoin. Another example of overlay networks is Omni and Counterparty that completely proposed new transaction syntax. Nxt is another cryptocurrency that built their own blockchain from scratch.

- *Smart contracts*: It is any actual contract written in programming code and by using computers it can be run. The most important element in the second generation of blockchain (Bitcoin 2.0) is the smart contract. To solve problems that are common and to reach agreements within a minimal trust, the smart contract is deployed and executed on the blockchain and is used by connected components.

  SamrtContract is an example of platforms that allows end users to build a self-executing contract on the Bitcoin blockchain. After being submitting and before being propagated to the network, the smart contract still can be updated. The scripting language used in the Bitcoin network does not support complex control flow, and it is limited expressiveness. Hence, smart contracts in this network are very simple. A blockchain-based platform called Ethereum was proposed to address the issue of supporting complex contracts. Ethereum started from scratch to build its own blockchain and to introduce a scripting language to write complex smart contracts.

2 BLOCKCHAIN SOFTWARE ARCHITECTURES

This section will address the variously proposed architectures for blockchain. Figure 1 shows a simple model of the blockchain. In Figure1 it can be seen how each block has a POW of the previous block that is forming the blockchain. The following subsections are a brief description of some proposed approaches that are based on blockchain invention.

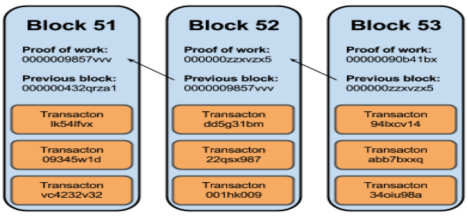

Figure 1: Example of Blockchain [4]

2.1 Cryptocurrencies

Blockchain has firstly utilised and introduced as mentioned above in the Bitcoin network. The Bitcoin network is a purely peer-to-peer decentralised electronic cash system created by Satoshi Nakatomo [5] in 2008. It is the first technology that successfully validate transactions without the need of a trusted third party. To validate transactions between the network's participants and to ensure the integrity of transactions, public key cryptography and digital signature have been utilised respectively. The use of these cryptographic mechanisms provide high data security principles (e.g. Integrity, Confidentiality and non-repudiation). The public key in Bitcoin is considered as participants' addresses where they can receive transactions, and the private key is considered as ownership credentials. Private keys are stored in digital wallets for each participant, and their coins are represented as digital signatures.

In the Bitcoin network, blockchain has been used as a public ledger where all transactions have ever occurred are stored. Transactions between participants are defined as a message and consist of three parts as follow.

1. *Signature:* The digital signature is signed by the owner of keys using the private key. Hence, the verifier can check that the message signed and came from the holder of the keys.

2. *Input:* It is a list of transactions' signatures already stored in the blockchain. The sender uses these signatures as a fund in the transaction.

3. *Output:* It is a list of the transactions that were funded by the input and how they should be distributed. The outputs must have the same number of the inputs in the Bitcoin network. The number of bitcoin in the inputs and the outputs in the bitcoin transaction must be the same. Figure 2 presents an overview of the bitcoin transactions.

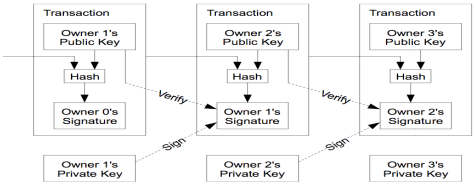

Figure 2: Bitcoin transaction overview [5]

Cryptocurrencies have shown that the new invention of blockchain is robustness, overcome the necessary of centralised trusted authority and might be suitable for enormous applications. Thus, blockchain has become a focus point of deploying it in some practical applications(e.g. Copyright management system, Software licence system, Reputation system, etc.). Table 1 shows a list of cryptocurrencies that used blockchain as a core of their architecture.

Cryptocurrencies	References (Websites)
Bitcoin[1]	https://bitcoin.org/
Peercoin	http://peercoin.net/
Colouredcoin	http://colouredcoins.org/
Omni	http://www.omnilayer.org/
Nxt	http://nxt.org/

Table 1: A list of cryptocurrencies based on blockchain

2.2 Smart Contracts Applications

Bitcoin has proved that blockchain technology is secure against several attacks, and its history is difficult to be changed, and it works without trusted third party.

Thus, Blockchain-based applications of things, not just cryptocurrencies have been started appearing. One of these applications is the contracts management system which is an example of smart contracts. In [6] the authors have proposed the first contract management (e.g.Digital management) that based on blockchain as they claim. In their solution, they replaced the POW puzzle with their puzzle called "Credibility". They assumed that the blockchain for the copyright management system must be expanded to make the contract as clear as, so they have proposed their solution based on the credibility that a contractor has. In their approach, they calculate how many numbers of parties, the contractor enter with into contracts. These numbers are called credibility score. To avoid fake contracts that contractors might introduce to gain more credibility ratings, their work combines two consensus methods; the credibility score and POS. POS is for storing the coins that are necessary to create the contract. In this blockchain model to create a block if a node runs one method mention above then the following node must run the other methods. Figure 3 shows the block generation methods of [6].

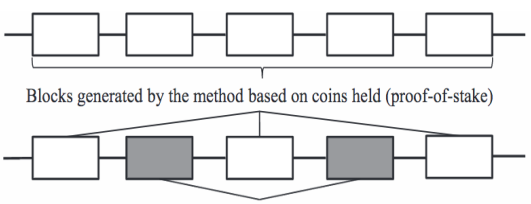

Figure 3: The blockchain generation methods in [6]

In 2015 Fujimura et al. in [7] proposed a new right management system based on blockchain technology. In their work, they have discovered a problem that might occur when applying this technology to the rights management system and proposed their solution. They found that the exchange of rights or licences information in rights management system might have videos and audios, whereas in cryptocurrencies is just currencies. They raised a question of how to treat videos and audios in the current blockchain. Figure 4 shows the overview of their system.

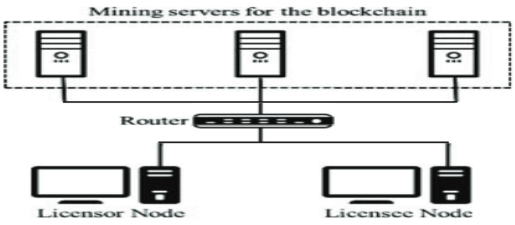

Figure 4: Fujimura et al.'s system overview

In Fujimura et al.'s system, the mining servers are utilised to solve the puzzle POW and to add a new block to the blockchain; three nodes are the smallest number that allowed maintaining the blockchain. The licensors and the licensee nodes are not for mining they just utilised the blockchain to receive and issue transactions. Another problem they have addressed which is the latency of adding a new block to the blockchain, based on Nakamoto to add a new block to the blockchain it takes ten minutes, and this is due to the difficulty of finding the nonce see [5] for a comprehensive explanation. They mitigate this problem by reducing the difficulty of POW.

In 2015, a new smart contract application based on blockchain named "recording contract" has been presented by Watanabe et al. [8]. This work aimed to prove that the agreement of contractors is obtained and to store the documents of contracts in the blockchain. Watanabe et al. found the transactions in cryptocurrencies are issued in a one-way direction, which is insufficient in recording contracts due to the need for confirmation on the part by the contract's parties. Also, "contractual documents are necessary to be archive by contractors. Current blockchain stores the hash value of document as a metadata which is not enough in contracts" Watanabe et al. said. Thus, they have expanded the current blockchain to overcome aforementioned issues in the current blockchain technology.

In Watanabe et al.'s protocol, to ensure the agreement of the contract, a transaction is used which contains the information of the contract, see Figure 5.

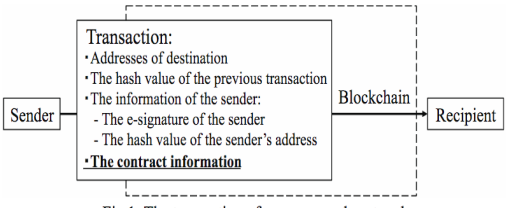

Figure 5: Watanabe et al.'s transaction protocol

To solve the first issue, contractors issue a chain of transactions, where each recipient presents his/her agreement to the contract, and at the end, the contract is returned to the contractor who generated the transaction. Then s/he verifies the agreement contain and issues a transaction to someone else as a trail of conformation. The second problem is mitigated by encrypting the contract and store it in the blockchain. The authors have used tow keys pairs one for e-signature and the other one to encrypt and decrypt the information of contracts.

Kishigami et al. in 2015 [9] deployed the blockchain technology in the digital content distribution system, which is considered a smart contract system. They claim the proposed system can only be operated by the holders of content rights. The system has three primary goals; the owner of the content has full control over everything, maintain the security and the simplicity and finally the system specifically targets high-resolution video(e.g. 4K or 8K). Authors' system is similar to the bitcoin system with two main differences. The first difference is the proposed system does not convey the money and the second one is the incentive. In bitcoin users (miners) are rewarded for solving the puzzle POW, which consumes their computational power, whereas this system does not have the incentive. Figure 6 shows the overview of the system and its components. As can be seen the system consists of 3 main components; Licensor, who issues to each owner a permission control and uploads files, Miners who are the core of the scheme and their functions are to generate, add and broadcast the blocks of the blockchain, and licensee who runs two applications one to get from the blockchain the right information and the other to play the 4K contents. This scheme has no intensive mechanism for mining computation power. The considered the intensive approach must be discussed in the business model.

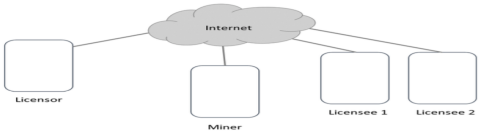

Figure 6: Kishigami et al.'s system overview

2.3 Reputation System Applications

The reputation system is a system that benefits from the blockchain technology. Some researchers have focused on this system and identified the limitations of the current state and tried to deploy blockchain on this system to solve identified limitations. This subsection will address some of the works have been carried out on this topic.

In 2015, Carboni [10] introduced the first blockchain-based reputation system. Carboni's scheme is ultimately deployed on top of bitcoin blockchain. Their scheme consists of five concepts; services S, which is a produced service or online consumed (e.g. Online games). Service Level Agreement SLA, which is the contractual obligation. Customers, Services Providers, Money transaction and Voucher which is linked to money transaction and has vote fees (3%) of this money and can have an incentive. The voucher must be digitally signed by the customer and the services provider, as this is the important concept behind it. Carboni's scheme works as following; the customer orders a service, then s/he sends the payment if satisfied then they leave feedback by either accept or not the incentive in the voucher. Completing the voucher transaction is like logically increase the positive feedback of the services. The total reputation score is the sum of vote fees for these services. Figure 7 illustrates the process of Carboni's scheme.

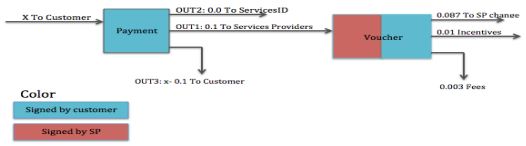

Figure 7: Carboni's scheme overview

The first generalised reputation scheme by Dennis et al. in 2015 that based on blockchain technology was introduced. This work aimed to solve today's current generation schemes' unsolved problems. In their scheme 0 and 1 is the only reputation scores are stored. The negative reputation is donated by 0 and the positive by 1 i.e. 1 if the user received the product they requested 0 otherwise. In this scheme authors just considered the data product, for instance, file signed with the private key of the user sent to the requester. After receiving the file, the hash of the file and a timestamp, as well as reputation score (0 or 1), is encrypted and sent to the miners as a transaction. Afterword, miners, send a nonce to both the user and the requester challenging them to concatenate the nonce with the file's hash and send them back to verifying the transaction and adding a new block to the chain. In this reputation system, the user controls the system and calculate scores based on a set of parameters identified by them. For instance, reputations on a particular network from users could be viewed by a user. The reputation score is given to the user based on the average of all their score. By doing this, they prevented the collusion attack. This scheme has been analysed by the authors and they claimed it sufficient and ready to be implemented and apply in the E-commerce system.

In 2016, Schaub et al. presented a new scheme based on the blockchain.

Schaub et al. claimed that the previous solution [10] is not a useable solution yet. For this reason, they found this solution, which based on their claim was Trustlessness, Suitability for e-commerce, Decentralisation, Anonymity preservation and Robustness. Schaub et al.'s scheme works as; firstly the customer rum particular function to calculate the reputation score of a services provider. If the customer is happy, s/he runs a function to create a public key derived from their pairs of key and keep it secret. The key will be used to mitigate token-theft. Then the transaction takes place, i.e. send the money and wait for the delivery. Next, a function is run by the customer to obtain a blind token from the services provider, who is required to have an enough balance to issue these token. Upon receiving, s/he verifies the token and unblinds them using the new public key. Finally, if the customer wishes to provide a feedback s/he should broadcast a message that contains the services provider address, the feedback either score or text, the received token, the signature of these and a pointer to the last review about the same provider by running an individual function. The calculation of the reputation score is done by finding the last block contains a review of the services provider then following pointers to retrieve all reviews. This work seems to be the most recent and robust solution.

2.4 Other Blockchain-based Application

In this subsection, a brief survey of different applications based on the blockchain technology (e.g. E-voting and Privacy-preserving app.) is conducted.

The E-voting system is a system that might benefit from blockchain due to the issues of the privacy and reliability of the current systems. In 2014, a new attempt to deploy and make use of the amazing invention of the blockchain was presented by Noizat. This scheme used the existing blockchain of the bitcoin for the log vote, and audit the result, Merkel Hash Tree (MHT) [14] for verification voters' list as well as block explore to check voters' accounts. Noizat's scheme has five steps to give a vote. The first step is named "Pre-election", in this step each voter is assigned a public key by the candidate and published everywhere. These keys are constructed as a tree using MHT, and the root is published. The second step is called "Check the list of voters", in this step a public key and a nonce are assigned for each voter by the election organisation. Each voter uses these keys to access his/her account. These keys are constructed as MHT and the root also publish. Any voter can verify the MHT root using his/her hashed public key. Due to the deployment of this system on the top of the bitcoin, each voter needs a balance to vote. Hence, voter balance is initialised at the registration time. For instance, if the voter is only allowed to choose one option, then his/her balance will be one. Voting is performed by creating digital signatures from the keys mentioned above; then a transaction is sent to the chosen candidate. After a period, the transaction is verified and added to the blockchain by the network miners. The next step is "votes counting", this is done by an implemented application which displays the result for the blockchain. The final step is "Post-election", in this step, the final result is published by collecting and calculating each candidate's balance. Although this a simple and based on existing technology, this work might

attract researchers in this area ”E-voting” to look at the possibility of using the blockchain on this topic.

An interesting new application based partially on the blockchain was presented in [15]. It focused on the user's data privacy by combining two storages blockchain and off-blockchain to construct a personal data management platform. Zyskind et al. addressed the user's data privacy breach issues in mobile platforms. In some mobile applications, users are required to give permissions to these applications to access their data. Upon giving these permissions, the user cannot change them late unless uninstalling those applications. Authors proposed a solution for these issues using both blockchain and off-blockchain to enable the user to have full control of the permissions. The following is the design of Zyskind et al. system. Two types of transaction are accepted by the blockchain; Access transactions and Data transactions. The Access transactions are used for access control and Data transaction for storage and retrieve the data. A user download and sign up for an application, then a new identity shared between the user and the application is stored and sent to the blockchain by the Access transactions. Any collection of data is encrypted using a shared key then sent to the blockchain. Afterward, it is redirected to off-blockchain by the blockchain which just stores a pointer to that data. The Data transaction is used by both entities to query the data using the pointer associated with it. For the services the blockchain checks both the digital signature as well as the permission whereas for the user only checks the digital signature. The user at any given time can alter and revoke the permissions associated with any services using the Access transactions. Figure 8 illustrates an overview of Zyskind et al. scheme.

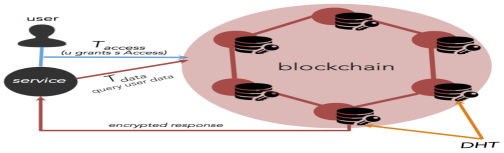

Figure 8: Zyskind et al. scheme overview

3 Conclusion

In this paper, a survey about blockchain software architectures was presented. Background about the blockchain and bitcoins was discussed, and some applications based on the blockchain technology that has been published were examined. Based on this survey, the blockchain technology could be suitable for a wide range of applications that is worth a research interest.

References

[1] *Crypto-currency market capitalizations*. URL: http://coinmarketcap.com/ (visited on 06/01/2016).

[2] Joseph Bonneau et al. "SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies". In: *Security and Privacy (SP), 2015 IEEE Symposium on*. IEEE. 2015, pp. 104–121.

[3] Florian Tschorsch and Björn Scheuermann. "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies." In: *IACR Cryptology ePrint Archive* 2015 (2015), p. 464.

[4] Jeff Herbert and Alan Litchfield. "A Novel Method for Decentralised Peer-to-Peer Software License Validation Using Cryptocurrency Blockchain Technology". In: *Proceedings of the 38th Australasian Computer Science Conference (ACSC 2015)*. Vol. 27. 2015, p. 30.

[5] Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*. 2008.

[6] Hiroki Watanabe et al. "Blockchain contract: Securing a blockchain applied to smart contracts". In: *2016 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE. 2016, pp. 467–468.

[7] Shigeru Fujimura et al. "BRIGHT: A concept for a decentralized rights management system based on blockchain". In: *Consumer Electronics-Berlin (ICCE-Berlin), 2015 IEEE 5th International Conference on*. IEEE. 2015, pp. 345–346.

[8] Hiroki Watanabe et al. "Blockchain contract: A complete consensus using blockchain". In: *2015 IEEE 4th Global Conference on Consumer Electronics (GCCE)*. IEEE. 2015, pp. 577–578.

[9] Junichi Kishigami et al. "The Blockchain-Based Digital Content Distribution System". In: *2015 IEEE Fifth International Conference on Big Data and Cloud Computing (BDCloud)*. IEEE. 2015, pp. 187–190.

[10] Davide Carboni. "Feedback based Reputation on top of the Bitcoin Blockchain". In: *arXiv preprint arXiv:1502.01504* (2015).

[11] Richard Dennis et al. "Rep on the block: A next generation reputation system based on the blockchain". In: *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE. 2015, pp. 131–138.

[12] Alexander Schaub et al. "A trustless privacy-preserving reputation system". In: ().

[13] Pierre Noizat. *Using the Bitcoin Blockchain for secure, independently verifiable, electronic votes*. 2014. URL: https://bitcoin.fr/public/divers/docs/Blockchain_Electronic_Votes_-_White_paper.pdf (visited on 05/17/2016).

[14] Ralph C Merkle. "Protocols for public key cryptosystems". In: *null*. IEEE. 1980, p. 122.

[15] Guy Zyskind et al. "Decentralizing Privacy: Using Blockchain to Protect Personal Data". In: *Security and Privacy Workshops (SPW), 2015 IEEE*. IEEE. 2015, pp. 180–184.

[16] Sunny King and Scott Nadal. “Ppcoin: Peer-to-peer crypto-currency with proof-of-stake”. In: *self-published paper, August* 19 (2012).

[17] Marc Pilkington. “Blockchain Technology: Principles and Applications”. In: *Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar* (2016).

[18] Xiwei Xu et al. “The blockchain as a software connector”. In: *Proceedings of the 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*. 2016.

[19] Christopher Natoli and Vincent Gramoli. “The Blockchain Anomaly”. In: *arXiv preprint arXiv:1605.05438* (2016).

[20] M Walport. “Distributed Ledger Technology: Beyond Blockchain”. In: *UK Government Office for Science, Tech. Rep* 19 (2016).